FRANK F. SOMMERS IV, ESQ. (SBN 109012)
ANDREW H. SCHWARTZ, ESQ. (SBN 100210)
SOMMERS & SCHWARTZ LLP
550 California Street
The Sacramento Tower, Suite 700
San Francisco, California 94104
Telephone: (415) 955-0925
Facsimile: (415) 955-0927

Attorney for Plaintiff,
NACIO SYSTEMS, INC.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

NACIO SYSTEMS, INC.	)	Case No.: C 07 3481 PJH
a Nevada corporation,	)	
	)	
Plaintiff	)	**DECLARATION OF PETER GARZA IN**
v.	)	**SUPPORT OF :**
	)	
HERBERT GOTTLIEB, an individual;	)	**1) PLAINTIFF'S APPLICATION WITHOUT**
SWIDENT, LLC, a California	)	**NOTICE FOR TEMPORARY RESTRAINING**
Limited liability corporation,	)	**ORDER RE PRESERVING EVIDENCE ; AND**
	)	
Defendants	)	**2) PLAINTIFF'S SECOND APPLICATION**
_______________________________	)	**FOR TEMPORARY RESTRAINING ORDER RE COPYRIGHT INFRINGEMENT AND SHORTENING TIME FOR LIMITED DISCOVERY**

I, Peter Garza, hereby make the following declaration under penalty of perjury under the laws of the United States. I declare that the facts stated herein are true, correct and within my own personal knowledge. If called as a witness and sworn I could and will competently testify to these facts.

1. I am a Senior Vice President with First Advantage Litigation Consulting ("FADV"), a firm specializing in computer forensics and electronic discovery. Prior to joining FADV I was the founder and President of EvidentData, Inc. ("EvidentData"), a computer forensics firm located in Rancho Cucamonga, California.

2. I completed a Master of Science in Information Systems at Claremont Graduate University in 2001. Between 1989 and 1999 I was employed as a Special Agent with the Naval Criminal Investigative Service ("NCIS") specializing in computer investigations and operations. I was involved in criminal and counterintelligence cases that resulted in forensic analysis of over 1000 computer systems.

3. I have attended training courses in computer forensics, computer investigations and computer system administration. I have developed and taught advanced training courses in computer crimes investigation for the Department of Defense and other Federal law enforcement agencies, including the Federal Bureau of Investigation ("FBI") and the Air Force Office of Special Investigations, as well as other local law enforcement agencies.

4. I have taught a graduate course in advanced computer forensics at California Polytechnic University at Pomona. From January 2001 to December 2002 I taught a course entitled, "Technical Recovery in Electronic Evidence" for the Computer Security Institute in San Francisco.

5. Since founding EvidentData I have worked as a computer forensics expert in hundreds of civil litigation cases. I have recovered computer evidence in cases which have included investigation of computer intrusions, theft of trade secrets and trademark infringement, along with criminal investigations for the FBI, the Securities and Exchange Commission and other state and local law enforcement agencies. A true and correct copy of my resume is attached hereto.

6. FADV and I have currently been retained to provide computer forensics consulting services by Nacio Systems, Inc. in the litigation entitled *Nacio Systems, Inc. v. Herbert Gottlieb et al,* U.S. District Court for the Northern District of California, case number C 07 3481 PJH. In many civil cases I have been involved in I have been appointed as a special master in electronic discovery or worked as an independent or consulting expert in computer forensics. I assisted in developing protocols which strive to identify relevant evidence while minimizing the intrusion into the producing party's privacy and which seek to protect attorney-client privileged information. A protocol which begins with a forensic backup of the relevant computer media and involves turning over data identified through forensic analysis by FADV to the producing parties for review has been effective in many cases to address such concerns. A forensic protocol which addresses concerns regarding privacy or privilege typically involves the following general steps:

a. Obtain an image backup of relevant computer media.

b. Apply review parameters on verified copies of image backups. These parameters are either agreed on by the parties or ordered by the court. They may involve running text search terms, reviewing file systems, analyzing metadata, reviewing e-mail, and other techniques.

c. Prepare responsive data for delivery to producing party in a format that allows for review and preparation of a privilege log.

d. Deliver responsive data to producing party for their review.

e. Deliver reviewed responsive data to requesting party.

7. Forensic analysis of computer media normally begins with obtaining a forensic backup of that media as soon as possible. A forensic backup is a true and accurate copy of the original media. If a proper forensic backup of the media is not taken to preserve the data, evidence may be intentionally or unintentionally lost. Simply starting a computer system by its normal boot process may cause deleted data to be overwritten and files to be updated or otherwise altered by the normal functions of the computer system. In addition, a sophisticated user wishing to obliterate data can delete data in a manner that is unrecoverable by forensic processes.

8. Using the normal delete function in Microsoft Windows, for instance, a user can delete a file, but the data is recoverable until it is overwritten by new data. The disk space used by the file is simply marked for reuse by new data. Once the space used by the file is reused to store new data, the prior file is unrecoverable. All that may remain is data about the deleted file and not the contents of the file. Small files with links to the original file, temporary copies of data from the file and printer copies of the file are examples of artifacts of data which may indicate the prior presence of the file but not all the contents of the deleted file. Only by obtaining a forensic backup of computer media can deleted data be preserved along with artifacts that may, at a minimum, show the prior presence of relevant data.

9. As explained above, in order to preserve all data on the relevant media a forensic backup must be preserved. FADV often works under protective orders requiring only authorized disclosure of data from electronic evidence analyzed. The evidence procedures followed by FADV are in accordance with proper evidence procedures used by federal, state and local agencies for which we have performed contract computer forensics work. FADV will comply with an appropriate protective order in obtaining the forensic backup, performing analysis and providing relevant and responsive data to the appropriate party as directed. I have often executed a declaration or undertaking on behalf of the staff under my direction or had each staff member execute such undertaking.

10. Occasionally, the type of inspection or seizure of data to be performed has required FADV to work with U.S. Marshals or private investigators to execute the inspection or seizure order at the premises of a producing party. The primary concern when entering a residence or business is the safety of all concerned. On occasions when law enforcement or private investigative personnel are assisting in the execution of a court order, FADV has established protocols for processing electronic evidence. Having appropriate investigative or law enforcement personnel minimizes the likelihood of problems, particularly in a person’s residence. With over 10 years experience as an agent with NCIS and in approximately 8 years of experience in civil cases, I have been involved in many data seizures. Executing the order professionally with the appropriate

support will help ensure safety and allow for an efficient acquisition of the appropriate data.

I declare under penalty of perjury under the law of the United States that the foregoing is true and correct and that this declaration was executed at Tampico, Tamaulipas, Mexico, on this ____ day of _________, 2006.

____

Peter Garza